Corr. to JP 2001-510970

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 :
H04Q 7/22, 7/32

A1

(11) International Publication Number: WO 99/04583

(43) International Publication Date: 28 January 1999 (28.01.99)

(21) International Application Number: PCT/GB98/02064

(22) International Filing Date: 13 July 1998 (13.07.98)

(30) Priority Data:
9715097.3 17 July 1997 (17.07.97) GB

(71) Applicant *(for all designated States except US)*: ORANGE PERSONAL COMMUNICATIONS SERVICES LIMITED [GB/GB]; St. James Court, Great Park Road, Almondsbury, Bristol BS12 4QJ (GB).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: FORD, Peter [GB/GB]; 18 Summers Mead, Yate, Bristol BS17 5RB (GB).

(74) Agents: MUSKER, David, C. et al.; R.G.C. Jenkins & Co., 26 Caxton Street, London SW1H 0RJ (GB).

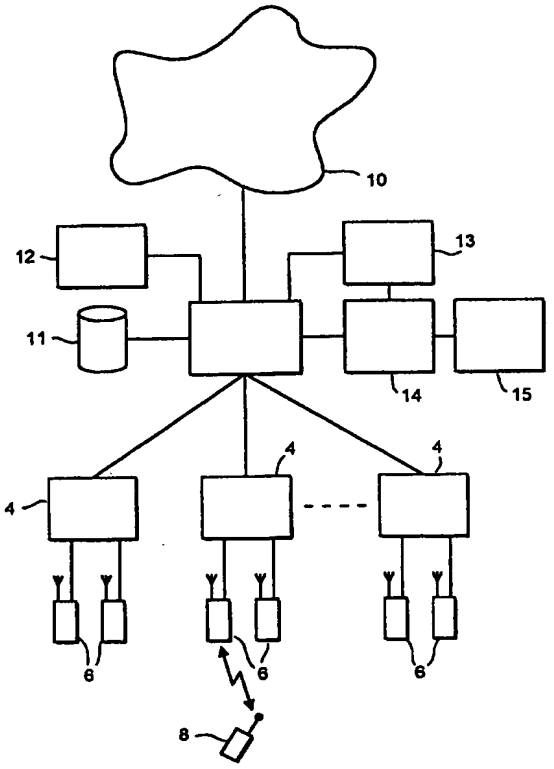
(81) Designated States: AL, AM, AT, AT (Utility model), AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, CZ (Utility model), DE, DE (Utility model), DK, DK (Utility model), EE, EE (Utility model), ES, FI, FI (Utility model), GB, GE, GH, GM, HR, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK (Utility model), SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: ENCRYPTED BROADCAST MESSAGES IN A CELLULAR COMMUNICATIONS SYSTEM

(57) Abstract

A method is described which provides functionality allowing mobile stations (8) of users having certain access rights to display messages broadcast on a common channel of a cell in a cellular telecommunications network in intelligible form. The messages, before broadcast, are encrypted using a predefined encryption key, and the mobile stations (8) having a corresponding access right are provisioned with the corresponding decryption key. Mobile stations lacking the appropriate access right are able to display a message, when received and picked up, only in encrypted, i.e. unintelligible, form. Some types of message broadcast within the cell on the same common channel are deemed general access messages, which are broadcast in unencrypted form and may be displayed in intelligible form by any mobile station (8) camped on to the cell in which the message is broadcast.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

ENCRYPTED BROADCAST MESSAGES IN A CELLULAR COMMUNICATIONS SYSTEM

This invention relates to a method of an apparatus for distributing and receiving information in a cellular telecommunications network, for example a GSM (Global System for Mobile communications) digital cellular radio network.

The GSM standard is defined in a set of technical specifications issued by the European Telecommunications Standards Institute (ETSI), and there are currently a number of mobile telecommunications networks operating in accordance with the GSM standard, and variants thereof, such as the DCS1800 standard.

One service provided is a service referred to as a cell broadcast (CB), or short message - cell broadcast (SMS CB), service. In this service, information in the form of pages of text is transmitted on a common channel (the cell broadcast channel, CBCH) of cells in the network. The transmission of pages is repeated at regular intervals, and users can store the information for retrieval and display by means of selective keystrokes on a mobile station, or may turn off the cell broadcast function so as not to store the information. The information is intended to include locality-specific information, such as lists of local facilities (hospitals, pharmacies, taxis, etc), local weather reports, local date/time indications, etc.

At present, however, the cell broadcast functionality, although provided for in current GSM-type networks and the mobile stations used in them, has not been widely implemented in practice, in probability at least partly due to the costs associated with assembling and disseminating information via the service.

In accordance with an aspect of the present invention there is provided a method of distributing information to users in a cellular telecommunications network comprising a mobile switching centre and a plurality of base stations transceiving in a plurality of cells of said network, said method comprising:

providing a plurality of mobile stations, each of said mobile stations having an associated information access status;

broadcasting a signal on a common channel of at least one cell of said network, said signal containing a limited access message in encrypted form, for general reception in said at least one cell;

enabling first mobile stations having a first information access status to decrypt and present said message to a user in unencrypted form when being served by said cell; and

preventing second mobile stations having a second information access status from presenting said message in unencrypted form to a user when being served in said cell.

An advantage of this aspect of the invention is that a user not authorised to access the information can only view the message in encrypted form and unintelligibly, whereas a user having access rights to the information is able to

view the message in decrypted and intelligible form services may be provided on a subscription basis. Some subscribers in the network may wish to have access to the information broadcast generally in the cell in addition to other services provided in the telecommunications network, such as voice call services, and will take out a subscription allowing access to the cellular information broadcasting service. Other users may not wish to receive the benefit of the information broadcast in the cell, and will take out a subscription, perhaps at lower cost, preventing them from accessing the information.

Preferably, the signal comprises a plurality of limited access messages each having a corresponding access right, the method comprising providing mobile stations with access rights, and enabling only mobile stations having an access right corresponding to a limited access message to present the limited access message to a user when being served in the cell. This allows the selection on a per user basis of the type of information a user is able to access, thus allowing a subscription to be individually tailored to a subscribers' needs.

The signal may also contain a general access message, the method comprising enabling both the first and second mobile stations to present the general access message to a user when being served in the cell. This allows both limited access messages and general access messages to be disseminated by broadcasts in cells of a cellular telecommunications system, allowing some information to be presented to any user irrespective of the subscription type held.

Preferably, alternative limited access messages are broadcast in cells located in different areas of the cellular telecommunications network, thereby tailoring the information within the messages to different localities and increasing the utility of the service.

In accordance with a further aspect of the invention there is provided apparatus for receiving information in a cellular telecommunications system, said apparatus comprising:

means for storing a decryption key;

means for receiving a message on a common channel in a cell of said cellular telecommunications system; and

means for decrypting said message using said stored decryption key; and

means for displaying said decrypted message to a user.

This aspect provides apparatus whereby a user may receive limited access messages on a common channel of a cell in the telecommunications system, and view the information in decrypted form, if the mobile station of the user is provided with the decryption key. A decryption key may be distributed only to cellular users having a predetermined subscription type.

An embodiment of the present invention will now be described, by way of example only, with reference to the accompanying drawings, wherein:

Figure 1 is a block diagram schematically illustrating a cellular telecommunications system;

Figure 2 is a block diagram schematically illustrating a cellular telecommunications mobile station;

Figure 3 illustrates a list stored in a cell broadcast centre in accordance with the present invention;

Figure 4 is a flow diagram illustrating functions carried out by the cell broadcast centre in accordance with the present invention;

Figures 5 and 6 illustrate data blocks broadcast in a cell in accordance with the present invention;

Figure 7 is a flow diagram illustrating functions carried out by a network management centre in accordance with the present invention;

Figure 8 illustrates a short message transmitted to a mobile station in accordance with the present invention;

Figure 9 illustrates functions carried out by a mobile station when displaying a cell broadcast message in accordance with the present invention;

Figure 10 shows an example of a display of a decrypted message in accordance with the present invention;

Figure 11 illustrates an example of a display of an encrypted message in accordance with the present invention; and

Figures 12 and 13 are flow diagrams illustrating encryption key updating procedures carried out in accordance with the present invention.

A GSM network, referred to as a public land mobile network (PLMN), is schematically illustrated in Figure 1. This is in itself known and will not be

described in detail. A mobile switching centre (MSC) 2 is connected via communication links to a number of base station controller (BSCs) 4. The BSCs 4 are dispersed geographically across areas served by the mobile switching centre 2. Each BSC 4 controls one or more base transceiver stations (BTSs) 6 located remote from, and connected by further communication links to, the BSC. Each BTS 6 transmits radio signals to, and receives radio signals from, mobile stations 8 which are in an area served by that BTS. That area is referred to as a "cell". A GSM network is provided with a large number of such cells, which are ideally contiguous to provide continuous coverage over the whole network territory. The radio signals are separated into a number of distinct communications channels. These include common channels and traffic channels. The traffic channels are used for point to point communications (voice calls, data calls, etc) with specific mobile stations. The common channels are received by all mobile stations being served by the cell and contain signalling and/or message data.

The mobile switching centre 2 is also connected via communications links to other mobile switching centres in the remainder of the mobile communications network 10, and to other networks such as a public service telephone network (PSTN), which is not illustrated. The mobile switching centre 2 is provided with a home location register (HLR) 11 which is a database storing subscriber authentication data including the international mobile subscriber identities (IMSIs) which are unique to each mobile station 8. An

IMSI consists of a mobile country code (3 decimal digits), a mobile network code (2 decimal digits) and a mobile subscriber code (up to 10 decimal digits) identifying a subscriber within a particular network. The IMSI is also stored in the mobile station in a subscriber identity module (SIM) (to be described below) along with other subscriber-specific information.

The mobile switching centre is also provided with a visitor location register (VLR), not shown, which is a database temporarily storing subscriber authentication data for mobile stations active in its area.

In addition, the MSC is connected to a cell broadcast centre (CBC) 12 for originating cell broadcast (CB) messages in the network, a short message centre (SMC) 13 for handling the transfer of point to point short messages within the network, a network management centre (NMC) 14 for performing management functions in the network, and a customer services system (CSS) 15 for performing customer service functions, including the updating of customer subscription data for example by manual input at workstations in the system.

Referring to Figure 2, a mobile station 8, more specifically a cellular mobile telephone, comprises a transmit/receive aerial 16, a radio frequency transceiver 18, a speech coder/decoder 20 connected to a loudspeaker 22 and a microphone 24, a processor circuit 26 and its associated memory 28, an LCD display 30 and a manual input port (keypad) 32. The mobile station 8 is connected to a removable SIM 34 via electrical contacts 35.

The SIM 34 connected to the mobile station has a SIM processor 36, for example a Hitachi H8 microprocessor, and SIM memory 38, which includes for example 16 kilobytes of mask-programmed ROM 38a containing the SIM operating system, 8 kilobytes of read/write EEPROM 38b for the non-volative storage of data items and 256 bytes of RAM for use by the SIM processor 36 during operations.

As described above, the SIM 34 is used for the storage and retrieval of data items by the processor 26 of the mobile station 8. The command set, data file structure and data coding format for data communicated via the interface between the mobile station processor 26 and the SIM processor 36 are all specified, in GSM technical specification 11.11.

Referring back to the network elements illustrated in Figure 1, the CBC 12 holds a set of cell broadcast messages to be broadcast within the network, and transmits them to the BSCs 4 in accordance with location areas which are predefined for each message type. Each cell broadcast message is provided with a unique message identifier (a 16 bit integer), which identifies the type of the message. The BSCs 4 then proceed to broadcast the message, via the respective BTSs 6, on their CBCHs. The CBCH protocols and the timing of the broadcasts are specified in GSM technical specification 05.02.

The CBC 12 holds a list as illustrated in Figure 3, specifying encryption keys for each type of message which is to be broadcast in encrypted form. For each such message, the key is listed against the message identifier. Each key is

a 16 bit integer and, since the message identifiers are also 16 bit integers, no two keys in the list need to be the same. The keys are used to encrypt a message using an XOR function as will be described below.

Figure 4 illustrates a procedure carried out by the CBC 12 when receiving a new message for transmission as a cell broadcast message. A new message may be provided in the CBC 12 for example by manual input on a workstation associated with the CBC, or may be provided on-line from a remote source.

When the CBC 12 receives the new message, which may be an update of a previous message stored for the same message identifier, the message is stored by the CBC 12 and any previous message stored for the same message identifier is overwritten, step 50.

Next, the CBC 12 checks, using the message identifier provided with the new message, whether the message identifier appears in the key list illustrated in Figure 3. If no key is held for that particular message identifier, the message will be made generally available by cell broadcast to all mobile stations served in the cells in which the message is to be distributed. The message is transmitted for broadcast to the relevant BSCs 4 in unencrypted form, step 52.

The cell broadcast message may consist of one or more (up to a maximum of 15) pages. Each cell broadcast page consists of 88 octets of information, consisting of a 6 octet header and 82 octets for message text. A 7 bit default character set is used, equating to up to 93 characters per page.

Figure 5 illustrates the manner in which each page of a cell broadcast message is transmitted in a cell by the BSC/BTS on the CBCH. The broadcast is divided into four blocks per page. The first block 100 contains 2 octets of data 108 indicating the serial number for the page, 2 octets of data 110 indicating the message identifier for the page, 1 octet of data 112 identifying the coding scheme used for the message text, and 1 octet of data 114 indicating the page parameter. The remaining 16 octets of data 116 contain the first part of the message text for the page.

The remaining 3 blocks 102, 104, 106 of the page broadcast consists entirely of message text, except each block is headed by a single octet of data 118 indicating the block type.

The serial number indicated in block portion 108 is a 16 bit integer which is used to identify a particular message. The serial number is updated when a message with a given message identifier is updated. The serial number consists of a 12 bit message code and a four bit update number, which are incremented according to message updates.

The message identifier in portion 110 is used to identify the type of message, as described above.

The coding scheme indicated in portion 112 is used to indicate the source language of the message, allowing a user to screen out any messages received in a language in which they are not conversant. The page parameter

indicated in portion 114 is used to specify the current page number within a message and the total number of pages within the message.

The message text for each page consists of up to 93 characters. If the message text within a page is shorter than 93 characters in length, the carriage return (CR) character is used to provide packing, thus bringing the total number of characters to 93. To maintain an integral number of octets, the remaining 5 bits are set to "0" as padding data at the end of the page.

The block structure illustrated in Figure 5 is that of a conventional cell broadcast message, and may be received and displayed by currently-available GSM-type mobile stations in receipt of the cell broadcast channel on which the message is broadcast.

Referring again to Figure 4, if on the other hand the CBC 12 detects the message identifier of the new message in the key list, the corresponding key is retrieved, step 54. The key is then used to encrypt the message, step 56, which is then transmitted to the appropriate BSCs 4, step 58. The encryption of step 56 is performed by applying an XOR function between the most significant 8 bits of the key and each odd-numbered message text octet in a page, and by applying the XOR function between the least significant 8 bits of the key and each even-numbered message text octet in a page, except the last such octet.

The pages broadcast by the BSCs 4 when receiving encrypted cell broadcast messages are of the form illustrated in Figure 6. Each page consists of the same components as the unencrypted page illustrated in Figure 5, namely

4 blocks each containing the various header portions. However, the majority of the message text is encrypted, as indicated by shading in Figure 6. The last octet of each page of message text, which contains the 5 bits of padding data, is left unencrypted, in order to protect the integrity of the padding data, which would be lost if encrypted. Each of the header portions is also transmitted in unencrypted form, to allow the proper reception and reading of the data in the header portions by all mobile stations 8.

In order to properly receive and present an encrypted cell broadcast message in intelligible form to a user, a mobile station 8 must be provisioned with the decryption key corresponding with the encryption key used to encrypt the message. With the XOR function as the encryption function, the encryption/decryption process is symmetric, and the same key used to encrypt the message is used to decrypt the message. This key is referred to herein as an encryption key when to be used to encrypt data, and a decryption key when to be used to decrypt data.

In order to provision the mobile station 8 with the decryption key, a remote provisioning procedure is used, involving a remote SIM updating (RSU) message being transmitted to the mobile station 8, such as described in European patent application no. EP-A-0562890, the contents of which are incorporated herein by reference, or using the "data download via SMS Point-to-point" (SMS-PP data download) procedure as described in GSM Technical Specification 11.14, "Specification of the SIM Application Toolkit for the

Subscriber Identity Module - Mobile Equipment (SIM-ME) Interface". The decryption keys are transmitted using a point-to-point data transfer protocol, such as the GSM-defined Short Message Service (SMS), over the radio interface to the mobile station 8 for storage in the SIM 34. The SIM 34 is provided with a cell broadcast decryption keys data field dedicated to the storage of cell broadcast decryption key data.

Figure 7 illustrates the procedures carried out by the NMC 14 in order to provision the mobile station 8 of a particular subscriber with decryption keys for each limited-access message type which the subscriber is entitled to have access to. The CSS 15 holds a record for the subscriber, indicating the access rights for that subscriber. These access rights are indicated by including in the subscriber record a list of the appropriate message identifiers for the message types which the subscriber should have access to. This access rights list may be updated and changed in the CSS 15.

In order to provision the mobile station 8 of the subscriber, the NMC 14 first interrogates the CSS 15 to determine the message access rights which are held for the subscriber, step 60. The NMC 14 also interrogates the HLR 11 in order to retrieve the IMSI of the subscriber, step 62. The NMC 14 also interrogates the CBC 12 to retrieve the decryption keys corresponding to each of the message identifiers indicated in the access rights details returned by the CSS 15, step 64. Next, each of the decryption keys returned by the CBC 12 is then itself encrypted by applying the XOR function between the 16 bits of the

decryption key and 16 predetermined bits of the subscriber's IMSI record, step 66. This is to ensure that the decryption key may only be used by a mobile station 8 having access to the subscriber's IMSI (which is stored in the subscriber's SIM 34).

Once the decryption keys are encrypted, the NMC 14 forwards an RSU message to the SMC 13 for transmission, via the radio interface, as an SMS message to the mobile station 8 of the subscriber. The SMS message is transmitted conventionally, via a dedicated data channel, to the mobile station 8. The RSU message has the form illustrated in Figure 8, and includes a header portion 70, the message identifiers for each message type to which the subscriber should have access to, the encrypted decryption keys, and alpha tags (alphanumeric identifiers) for use by the subscriber to readily identify each of the message types. The header portion 70 includes a flag indicating that the SMS message is an RSU message, and a command indicating that the contents of the message are to be stored in the cell broadcast decryption keys data field.

On receipt of the SMS message, the mobile station forwards it for storage as an SMS message to the SIM 34. However, since the message has an RSU flag, the SIM processor 36 notes that the message is an RSU message, and updates the cell broadcast decryption keys data field in the SIM 34 with the message identifiers, the corresponding encrypted keys, and the corresponding alpha tags contained in the RSU message. The mobile station is now provided with the capability to decrypt all encrypted cell broadcast messages having

message identifiers corresponding to those stored in the cell broadcast decryption keys data field.

A user of the mobile station may, by appropriate keystrokes on the keypad 32, select cell broadcast messages which the mobile station is to pick up and store for possible display by the user. The user may display the alpha tags for the message types of limited access messages, in order to aid the selection of the limited access message types which the user wishes to have displayed. The user is also able to select the message identifiers for message types of general access messages, and for message types of limited access messages which the mobile station has no decryption keys.

When a cell broadcast message is received by the mobile station 8 which has a message identifier of the type selected for possible display by the user, and no message is yet stored for the message identifier, the mobile station 8 picks up the message and stores the message in a cell broadcast message data field provided in the SIM 34. If the SIM 34 already has a message stored for the message identifier in the cell broadcast message, the mobile station 8 checks the serial number of the message to determine whether it has been updated. If so, the mobile station overwrites the previously-stored message in the SIM 34 with the updated message. Otherwise, the mobile station 8 ignores the contents of the cell broadcast message.

When a cell broadcast message is newly picked up and stored, the user is prompted, for example by an audio tone or by a particular icon on the LED

display 30 of the mobile station 8, to indicate that a cell broadcast message is ready to be displayed. The mobile station then performs the procedures illustrated in Figure 9.

The mobile station first waits for input by the user requesting the message to be displayed. On receipt of such input, the mobile station checks whether it is currently camped on its home network (HPLMN). If the mobile station is camped on a network which is not its home network, the mobile station proceeds directly to display the stored message. If the message is encrypted, the encrypted message is displayed in a form unintelligible to the user, step 78, as the message is of the limited access type and access to the information is denied to the subscribers of other networks. If the message however is unencrypted, i.e. of the general access type, the message is displayed in an intelligible form, step 80.

If the mobile station is camped on its home network, the mobile station checks whether the SIM 34 has the cell broadcast decryption keys data field provided in accordance with this invention. If not, the mobile station proceeds once again to either display an encrypted message, step 78, or an intelligible message, step 80, depending on the access type of message broadcast.

If the SIM 34 currently in the mobile station does have the cell broadcast decryption keys data field, the mobile station proceeds to interrogate the SIM 34 to check whether the message identifier of the stored message is present in the cell broadcast decryption keys field. If not, the message received may be of a

general access type, and the message is displayed by the mobile station 8 in intelligible form, step 80. Otherwise, the message is of a limited access type to which the user has no access rights. The message is then displayed by the mobile station 8 in encrypted, i.e. unintelligible form, to prevent receipt of the information in the message by the user, step 78.

If the message identifier of the stored message is present in the cell broadcast decryption keys data field on the SIM 34, the mobile station 8 proceeds to retrieve the encrypted decryption key corresponding to the message identifier of the stored message, along with the subscriber's IMSI, from the SIM, step 82.

With the encrypted decryption key and the IMSI, the mobile station 8 performs the reverse of the encryption process carried out in the NMC 14, to obtain the original decryption key, step 84. This decryption is carried out by performing an XOR function between the 16 bits of the encrypted decryption key and the same set of 16 predetermined bits from the subscriber's IMSI used in the encryption process.

The mobile station 8 then proceeds to decrypt the stored message, by performing the reverse of the encryption process carried out in the CBC 12 when generating the encrypted cell broadcast message. Namely, the mobile station performs the XOR function between the 8 most significant bits of the decryption key and each odd-numbered message text octet, and between the 8 least significant bits of the decryption key and each of the even-numbered

message text octets, except for the last octet in each page (which was originally not encrypted). This returns the original cell broadcast message text, which is then displayed on the LCD display 30 of the mobile station, step 88, in a form intelligible to the user.

Figure 10 illustrates an example of an original cell broadcast message, consisting of one page containing 89 message text characters and 4 carriage return (text padding) characters. This message is encrypted as described in relation to Figure 4, and after receipt and storage by the mobile station may be displayed in accordance with the procedure shown in Figure 9.

If the mobile station has been provisioned with the corresponding decryption key, the message may be displayed in its original form as illustrated in Figure 10.

If however the mobile station has not been provisioned with the appropriate decryption key, the message will appear as illustrated in Figure 11, as a pseudo-random character set.

Because the number of bits of the encryption key is not equal to, nor a multiple of, the number of bits used per character in coding the text, there is no direct correspondence between any one of the original characters and the characters displayed in the encrypted text. In this case, the coding scheme used for the text characters utilises 7 bits per character, and the encryption keys contain 16 bits. Of course, other combinations of text character coding length and encryption key length may be used to similar effect.

To ensure the long-term security of the encryption method used for limited access messages, the encryption keys used to encrypt the message texts will periodically be altered. Figure 12 illustrate a procedure carried out by the CBC 12 to update a particular encryption key. The CBC 12 first randomly generates a new 16 bit encryption key, step 90, and overwrites the previously-stored encryption key in the list illustrated in Figure 3 for the message identifier in question, step 91. Next, the CBC 12 proceeds to retrieve the message previously stored for the message identifier in question, step 92, and proceeds to encrypt the message with the newly generated encryption key, step 93. This encryption process is identical to that carried out when the message was originally received by the CBC 12 as described in relation to Figure 4, of course using a different encryption key. Once the message is encrypted, the new cell broadcast message is forwarded to the appropriate BSCs 4, step 94, for broadcast by the BTSs 6 on their CBCHs to mobile stations 8 receiving the cell broadcast channel in the cells served by the BSCs 4 in question.

Once a new encryption key has been generated in the CBC 12, and the corresponding cell broadcast message has been encrypted with the newly-generated key, the mobile stations 8 of users having access rights to the same message type must be provisioned with the new decryption key.

The first step of provisioning the mobile stations 8 of the appropriate subscribers with new decryption keys generated in the CBC 12 is the procedure carried out in Figure 13. First, the CSS 15 receives from the CBC 12 a list of

message identifiers for the messages for which the decryption keys have been updated, step 95. The CSS 15 then proceeds to search its store of subscription records for the message identifiers on the updated decryption keys list, in order to determine which subscriptions require updated decryption keys, step 96. The CSS 12 then constructs a list of such subscriptions, which are forwarded to the NMC 14 to allow the NMC 14 to perform the appropriate provisioning procedures, step 97. The NMC 14 then proceeds to perform the procedure described in relation to Figure 7 for each subscription appearing on the list received from the CSS 15. This results in the mobile stations of each such subscription receiving a new RSU message containing updated decryption keys, in encrypted form, for message types to which the subscriber has access. These decryption keys are suitable for use in decrypting messages encrypted with the newly-generated encryption keys.

The encryption/decryption mechanism utilised in the above-described embodiment utilises the two-way encryption/decryption character of the XOR function, and is sufficiently secure for use in relation to many types of information. However, it will be appreciated that other two-way encryption/ decryption mechanisms, for example using symmetric or public/private encryption/decryption keys, may be utilised to provide more (or less) secure encryption/decryptionmechanisms.

In the above-described embodiment, the general-access messages are not subject to the XOR function used in the encryption/decryption process.

However, it would also be possible to subject the message to the XOR function using a "free" key of the form of 16 bits of "0", which results in a message coding which is identical to the original message coding. This XORing with the "free" key may be performed in the CBC 12 when "encrypting" a general access message, and/or by the mobile station 8 when "decrypting" a general access message. In effect, no encryption or decryption would take place.

In the above-described embodiment, the mobile station 8 performs the decryption of the cell broadcast message text. This requires the mobile station itself to be customised, in relation to currently existing mobile station types, in order to allow the mobile station to present the encrypted cell broadcast messages in plain text form. In a further embodiment, a standard mobile station, such as a GSM (Phase 2+) mobile station supporting the SIM Toolkit as described in GSM Technical Specification 11.14, may be used. In this further embodiment, the functionality for decrypting encrypted cell broadcast messages is contained in the SIM 34 itself, the SIM 34 being SIM Toolkit enabled.

In order to avoid repetition, it should be understood that the functionality described in relation to each of Figures 3, 4, 7, 8, 12 and 13 is intended to apply equally in relation to 13. This embodiment differs primarily from the first-described embodiment in that the special cell broadcast coding scheme illustrated in Figure 6 is not necessary, a conventional "data download via SMS-CB" coding scheme being used instead, and in that the procedure illustrated in Figure 9 is not carried out by the mobile station, the mobile station

instead passing "data download via SMS-CB" messages directly to the SIM, and subsequently being instructed by the SIM (the SIM being proactive) to display a plain text version of a cell broadcast message received in encrypted form.

Referring to Figure 4, in this embodiment any suitable type of encryption technique may be used in step 56. This may be the XOR function previously described, or other encryption techniques such as DES, RSA, etc.

In place of the coding scheme illustrated in Figure 6, in this embodiment each of the BSCs 4 broadcasting encrypted cell broadcast messages formats the encrypted message as a "data download via SMS-CB" message, the encrypted message being included in the cell broadcast page along with an identifier for the key used to encrypt the message. The cell broadcast message includes a cell broadcast message identifier, which specifies the type of content contained in the cell broadcast page, and a transfer protocol identifier indicating that the message type is "SIM data download".

In addition to the field dedicated to containing decryption keys, which may be populated by means of RSU procedures as described above, the SIM 34 contains a Cell Broadcast Message Identity for Data Download (CBMID) data field, as described in GSM Technical Specification 11.11, which holds data identifying the message content types the subscriber wishes the mobile station 8 to accept. Furthermore, the SIM 34 includes an application programme, which

may for example be stored in ROM or EEPROM on the SIM, for performing decryption and controlling the display of the mobile station 8.

When the mobile station receives the cell broadcast download message, the mobile station 8 first queries the CBMID data field of the SIM to determine whether the message ID received for the cell broadcast message is currently selected by or for the subscriber. If a corresponding entry is found in the CBMID data field, the mobile station 8 transparently passes the cell broadcast page to the SIM 34 using a "cell broadcast download to SIM" command.

Reception of the cell broadcast download command by the SIM 34 causes the SIM to analyse the contents of at least a portion of the cell broadcast page, wherefrom it is determined whether the cell broadcast page contains an encrypted message. If so, the stored programme is invoked in order to decrypt the message, using the appropriate decryption key stored in the dedicated decryption keys field. Once the message is decrypted, the SIM passes the plain text message to the mobile station in a "display text" command, in response to which the mobile station 8 displays the plain text message.

In addition to decrypting the encrypted message and commanding the mobile station 8 to display the plain text message, the SIM application programme may also perform other processes in response to data received in the cell broadcast message, such as updating the contents of the CBMID data field to select new message types, on behalf of the subscriber, which the mobile station 8 should accept and handle.

As will be appreciated, in this embodiment, if a subscriber is not authorised to receive a limited access message in plain text form, the SIM may either not contain an appropriate decryption key for the message or may be at least temporarily configured by the network operator so as not to conduct the procedure described above. Instead of the procedure described above, the SIM may act in one of a variety of alternative manners. For example, the SIM may command the mobile station 8 either to present the message to the user in encrypted form or to display an access-denied message, or may simply not any display on the mobile station, in response to a cell broadcast message containing an encrypted message which is of a type nevertheless selected by the subscriber.

The functionality for the provision and processing of encrypted cell broadcast messages may thus be contained entirely within the mobile communications network and on the SIM 34, and standard (e.g. GSM Phase 2+) handsets may be used without modification.

It will be appreciated that various modifications and variations may be employed in relation to the above-described embodiments.

The provisioning of the mobile stations with decryption keys via the air interface, using the RSU-type short messages, has the advantage that no action is required on the subscriber's behalf in order to provision the SIM 34 of the mobile station 8 with the decryption keys. However, the decryption keys, preferably encrypted using the subscriber's IMSI, or such like, as described, may be transmitted to the user by other methods, for example by mail. An

alternative functionality of the mobile station 8 would allow the encrypted decryption keys to be manually input to the mobile station for storage in the cell broadcast decryption keys data field in the SIM 34.

Other information access prevention mechanisms to those described above could also be employed, such as the remote enablement/disablement(for example using RSU messages) of a decryption function on the mobile station, or of the cell broadcast receiving function on the mobile station.

In the above-described embodiments, the SIM 34 is in the form of a module electrically connected to the mobile station 8. However, the SIM may be embodied in an entirely separate module, such as a contactless smartcard transmitting data to and from the mobile station via a radio link.

Finally, although the above-described embodiments relate to a method and apparatus utilised in a GSM-type network, the present invention may of course be realised in other types of cellular telecommunications networks, whether using TDMA, CDMA, or other types of radio interface protocols.

It is envisaged that further modifications and variations may be employed without departing from the scope of the present invention.

CLAIMS

1. A method of distributing information to users in a cellular telecommunications network comprising a mobile switching centre and a plurality of base stations transceiving in a plurality of cells of said network, said method comprising:

providing a plurality of mobile stations, each of said mobile stations having an associated information access status;

broadcasting a signal on a common channel of at least one cell of said network, said signal containing a limited access message in encrypted form, for general reception in said at least one cell;

enabling first mobile stations having a first information access status to decrypt and present said message to a user in unencrypted form when being served by said cell; and

preventing second mobile stations having a second information access status from presenting said message in unencrypted form to a user when being served in said cell.

2. A method according to claim 1, wherein said first mobile stations are provided with a decryption key for said message.

3. A method according to claim 2, wherein said decryption key is held in a removable module which may be used in association with any of a plurality of mobile stations.

4. A method according to claim 3, wherein said message is decrypted in said removable module.

5. A method according to claim 2 or 3, wherein said signal contains padding data accompanying a portion of said message, and said portion is contained in said signal in unencrypted form.

6. A method according to any preceding claim, wherein said signal comprises a header portion containing a message identifier accompanying a message and said method comprises enabling both said first and second mobile stations to read said message identifier.

7. A method according to any of the preceding claims, wherein status data defining said information access status is stored in a removable module of a first mobile station.

8. A method according to claim 7, wherein said status data comprises a decryption key.

9. A method according to claim 8, wherein said decryption key is stored in said removable data store in encrypted form.

10. A method according to claim 9, wherein said decryption key is decrypted by said first mobile station using a data string specific to said removable module.

11. A method according to claim 10, wherein said data string is a subscriber identifier used in said cellular telecommunications network.

12. A method according to any of claims 7 to 11, further comprising transmitting said status data to said first mobile station via a radio interface in said cellular telecommunications network.

13. A method according to any preceding claim, wherein said signal comprises a plurality of limited access messages each having a corresponding access right,

said method comprising providing said mobile stations with said access rights and enabling only mobile stations having an access right corresponding to a limited access message to present said limited access message to a user when being served in said cell.

14. A method according to claim 13, comprising providing each of said first mobile stations with a selection of said access rights in accordance with a subscription held for each first mobile station respectively.

15. A method according to claim 13 or 14, further comprising storing encryption keys for each of a plurality of limited access message types, and encrypting each said limited access message using an encryption key in accordance with its respective message type.

16. A method according to any of claims 13 to 15, comprising storing a plurality of subscription records, each said subscription record comprising access right data defining said access rights.

17. A method according to claim 16, comprising altering said access right data for a subscription record to alter the type of limited access messages a user is able to receive intelligibly.

18. A method according to any preceding claim, wherein said signal contains a general access message, and wherein said method comprises enabling both said first and second mobile stations to present said general access message to a user when being served in said call.

19. A method according to claim 19, wherein said common channel is a cell broadcast channel of a GSM-type communications system.

20. A method according to any preceding claim, wherein alternative limited access message(s) are broadcast in cells located in different areas of said cellular telecommunications network.

21. Apparatus for receiving information in a cellular telecommunications system, said apparatus comprising:

means for storing a decryption key;

means for receiving a message broadcast on a common channel of a cell of said cellular telecommunications system; and

means for decrypting said message using said stored decryption key; and

means for displaying said decrypted message to a user.

22. Apparatus according to claim 21, wherein said storage means is part of a removable module.

23. Apparatus according to claim 21 or 22, wherein said displaying means is arranged to display a message in decrypted form when a decryption key for said message is held in said storage means, and to display said message

in encrypted form when no decryption key for said message is held in said storage means.

24. Apparatus according to claim 21, 22 or 23, wherein said decryption means is part of a removable module.

25. A cellular mobile telephone according to claim 21, 22, 23 or 24.

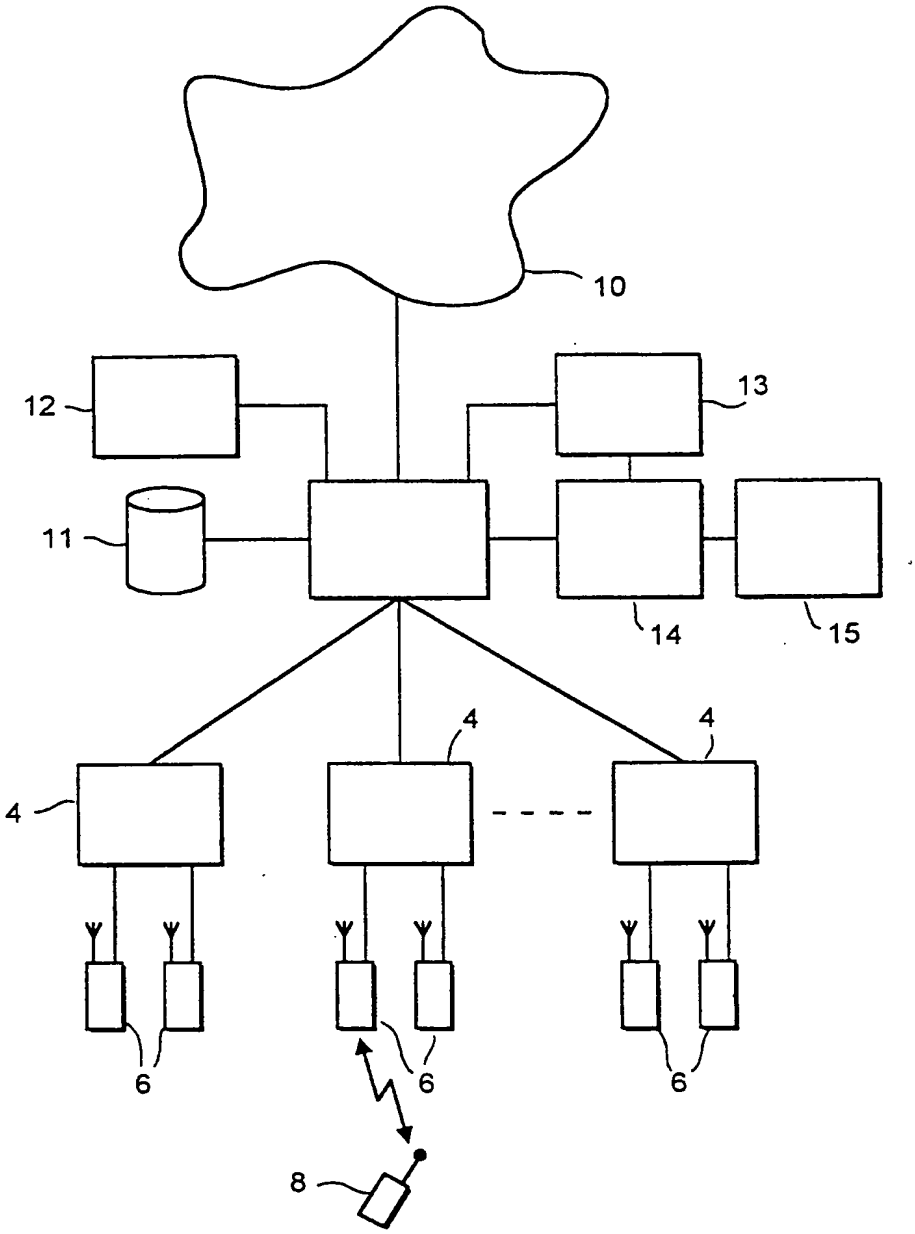


FIG. 1

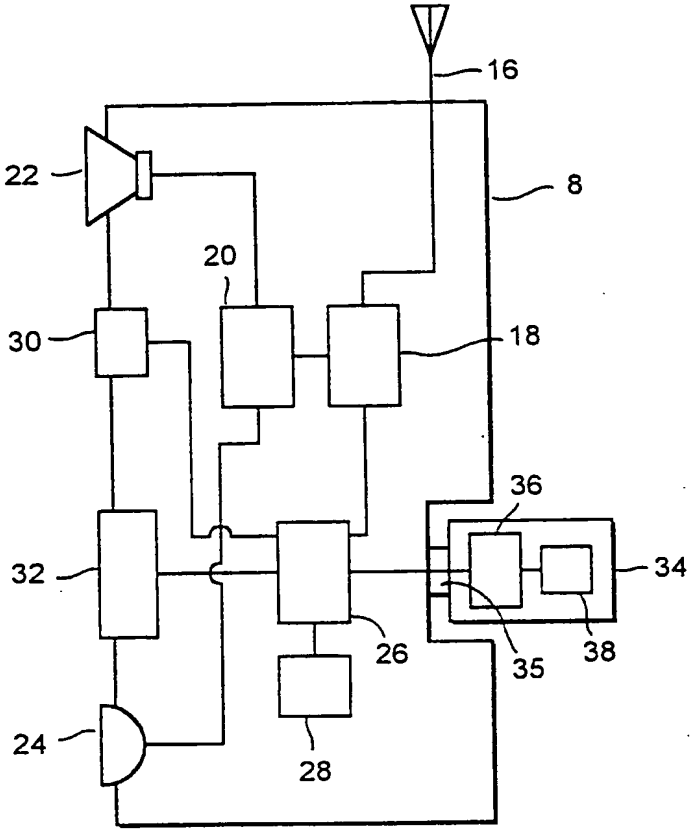


FIG. 2

MESSAGE IDENTIFIER	KEY
- - - - - - - - - - - - - - -	- - - - - - - - - - - - - - -
- - - - - - - - - - - - - - -	- - - - - - - - - - - - - - -
. . .	. . .
- - - - - - - - - - - - - - -	- - - - - - - - - - - - - - -

FIG. 3

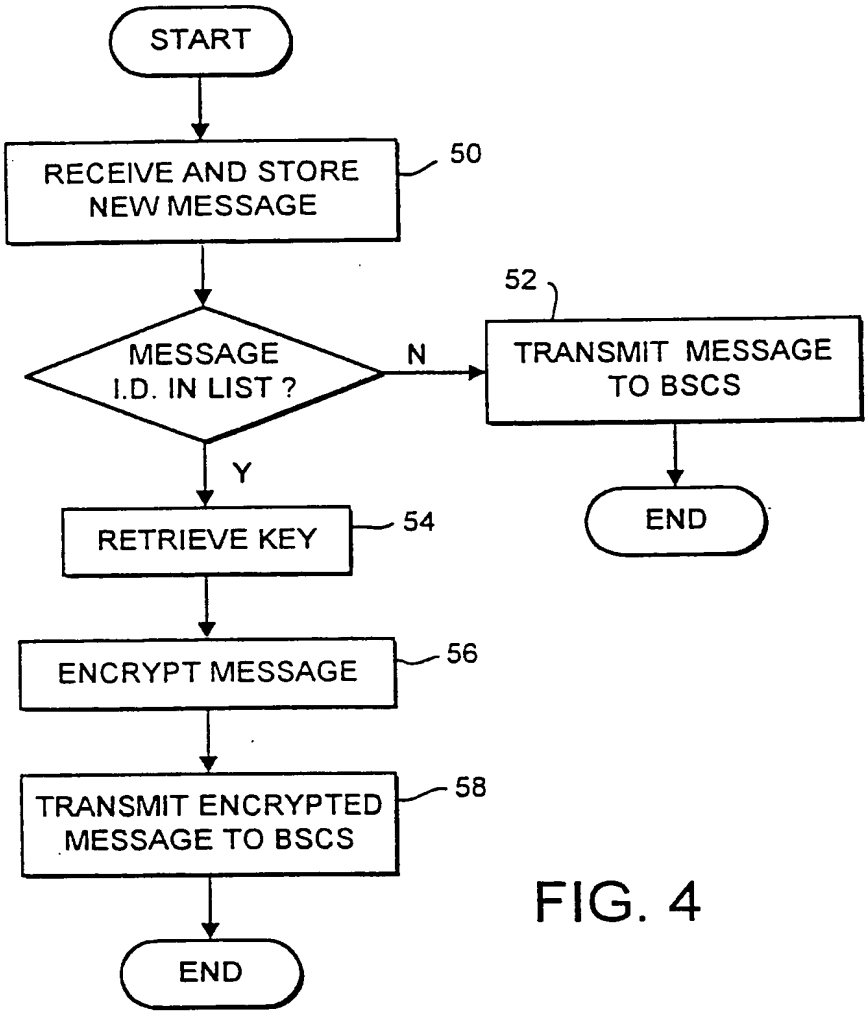

START
RECEIVE AND STORE NEW MESSAGE
50
MESSAGE I.D. IN LIST ?
N
52
TRANSMIT MESSAGE TO BSCS
END
Y
RETRIEVE KEY
54
ENCRYPT MESSAGE
56
TRANSMIT ENCRYPTED MESSAGE TO BSCS
58
END

FIG. 4

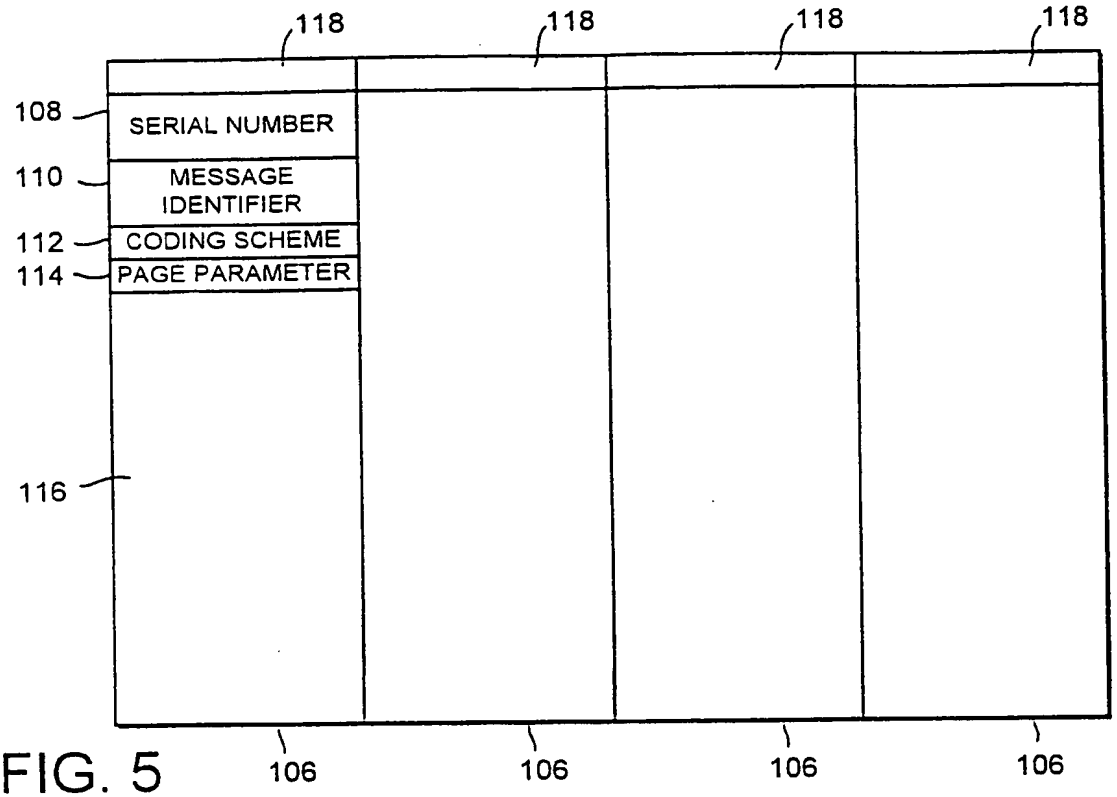

118
118
118
118
108
SERIAL NUMBER
110
MESSAGE IDENTIFIER
112
CODING SCHEME
114
PAGE PARAMETER
116
106
106
106
106

FIG. 5

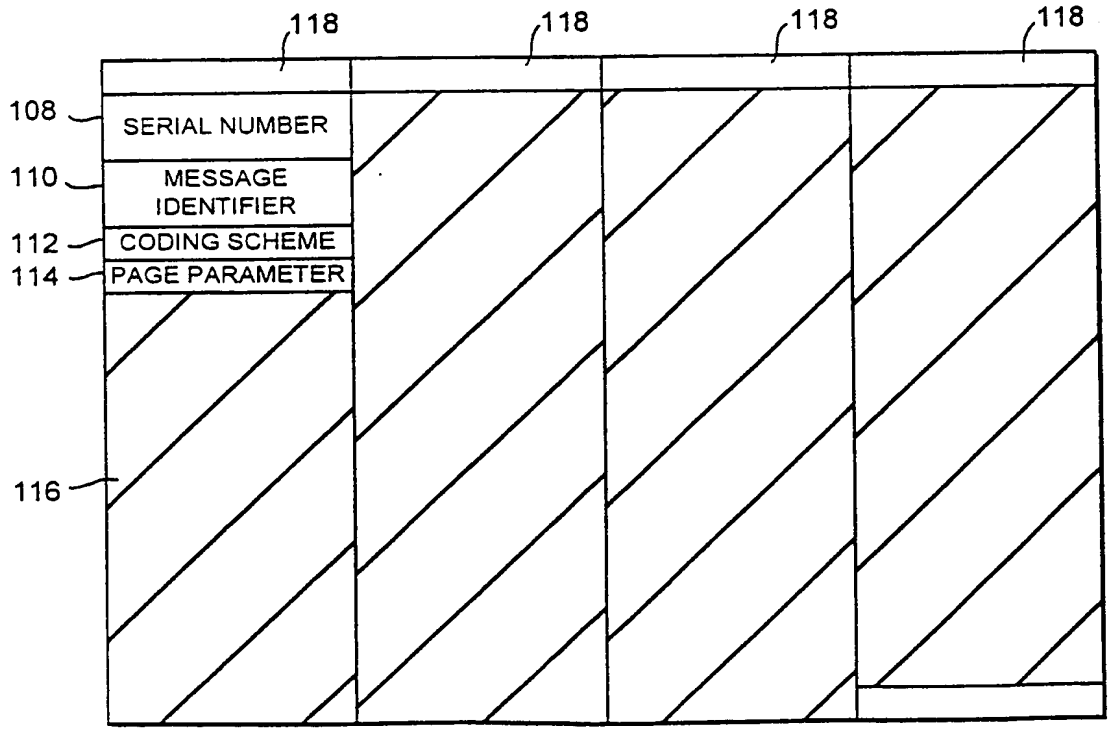

118
118
118
118
108
SERIAL NUMBER
110
MESSAGE IDENTIFIER
112
CODING SCHEME
114
PAGE PARAMETER
116

FIG. 6

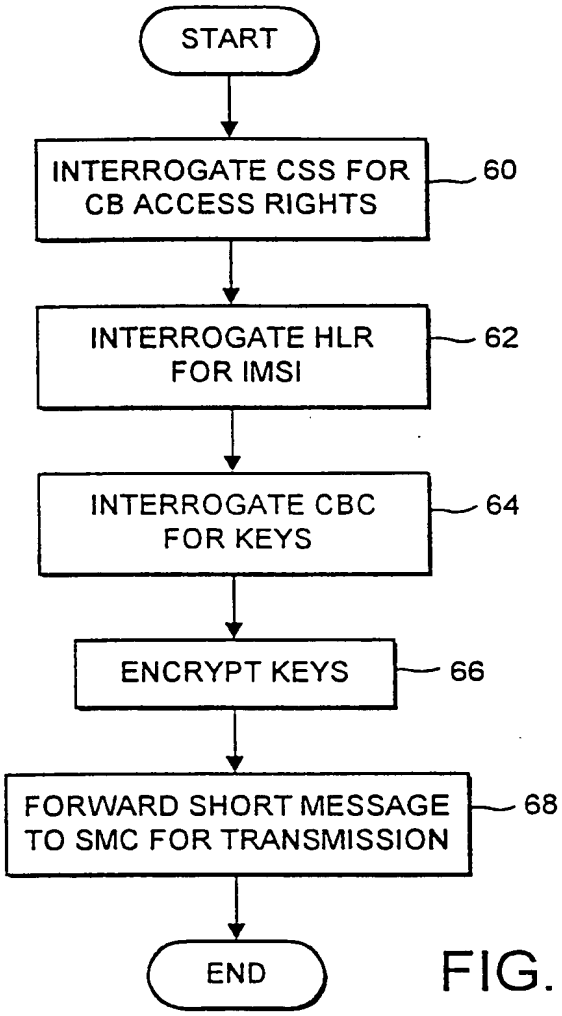

START
INTERROGATE CSS FOR CB ACCESS RIGHTS
60
INTERROGATE HLR FOR IMSI
62
INTERROGATE CBC FOR KEYS
64
ENCRYPT KEYS
66
FORWARD SHORT MESSAGE TO SMC FOR TRANSMISSION
68
END

FIG. 7

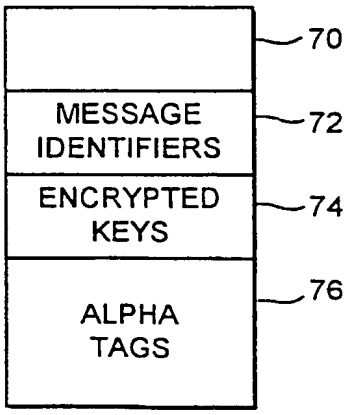

70
MESSAGE IDENTIFIERS
72
ENCRYPTED KEYS
74
ALPHA TAGS
76

FIG. 8

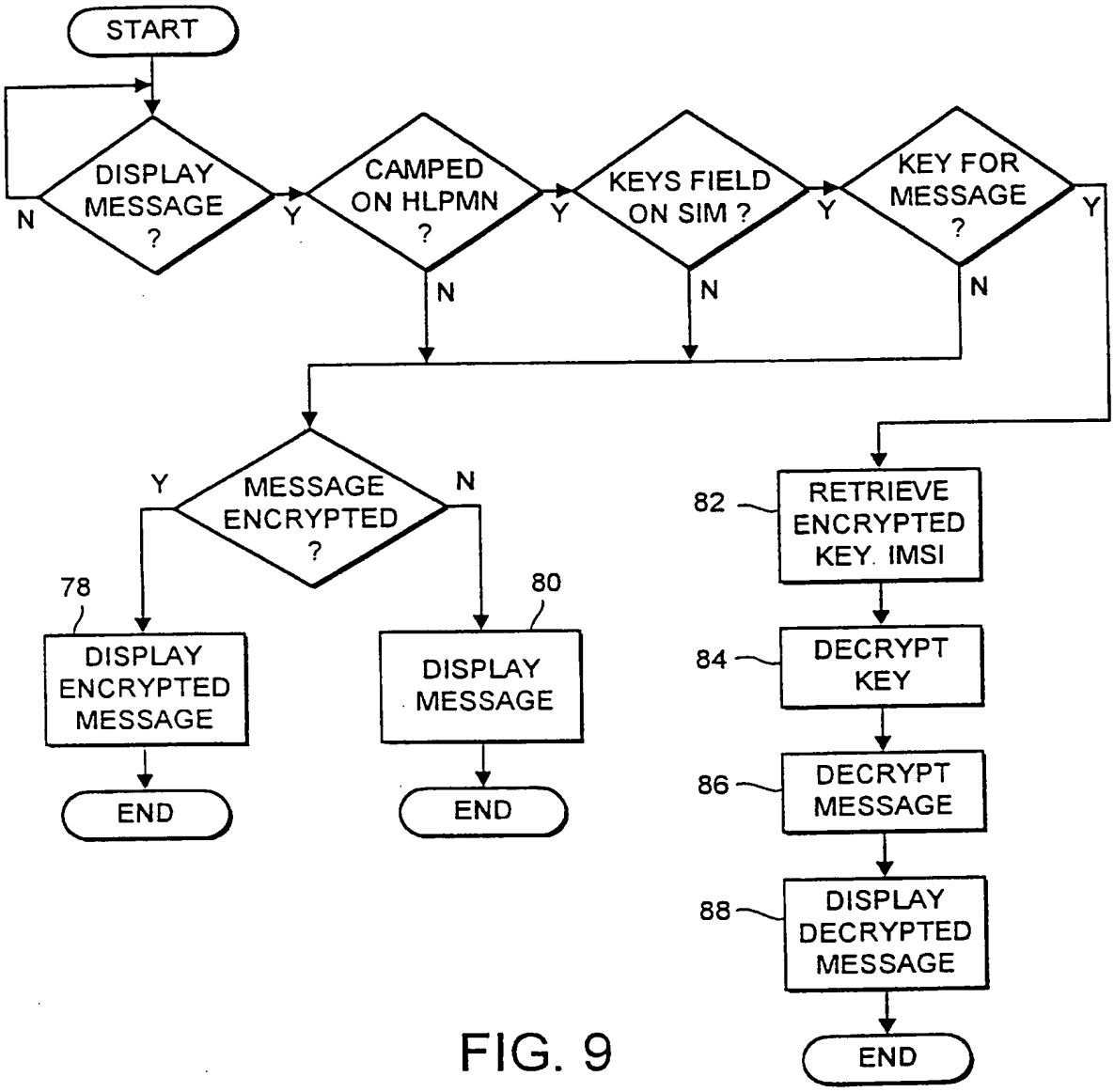

START
DISPLAY MESSAGE ?
N
Y
CAMPED ON HLPMN ?
Y
KEYS FIELD ON SIM ?
Y
KEY FOR MESSAGE ?
Y
N
N
N
MESSAGE ENCRYPTED ?
Y
N
78
DISPLAY ENCRYPTED MESSAGE
END
80
DISPLAY MESSAGE
END
82
RETRIEVE ENCRYPTED KEY. IMSI
84
DECRYPT KEY
86
DECRYPT MESSAGE
88
DISPLAY DECRYPTED MESSAGE
END

FIG. 9

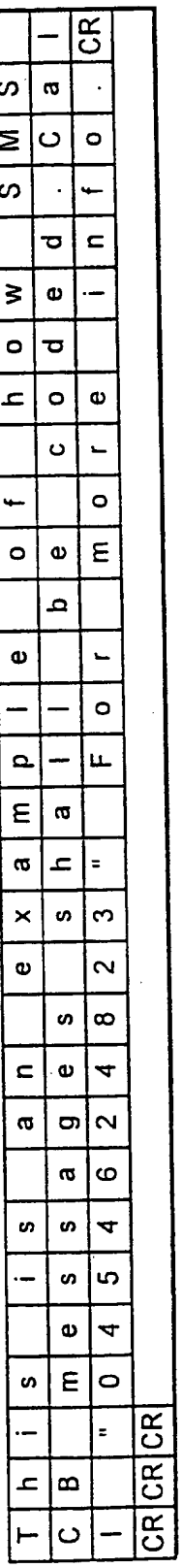


FIG. 10

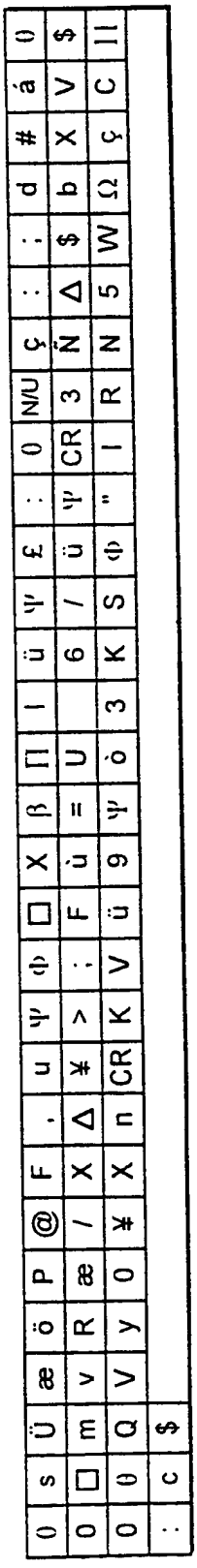


FIG. 11

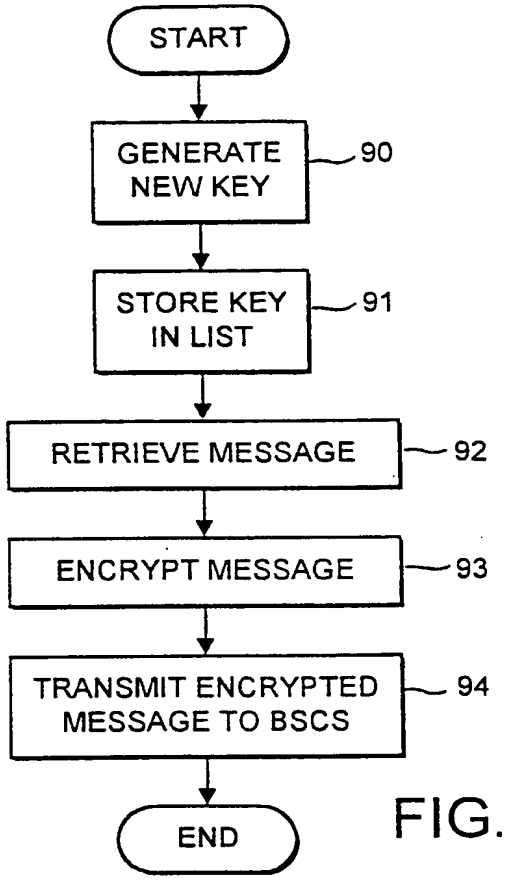

START
GENERATE NEW KEY
90
STORE KEY IN LIST
91
RETRIEVE MESSAGE
92
ENCRYPT MESSAGE
93
TRANSMIT ENCRYPTED MESSAGE TO BSCS
94
END

FIG. 12

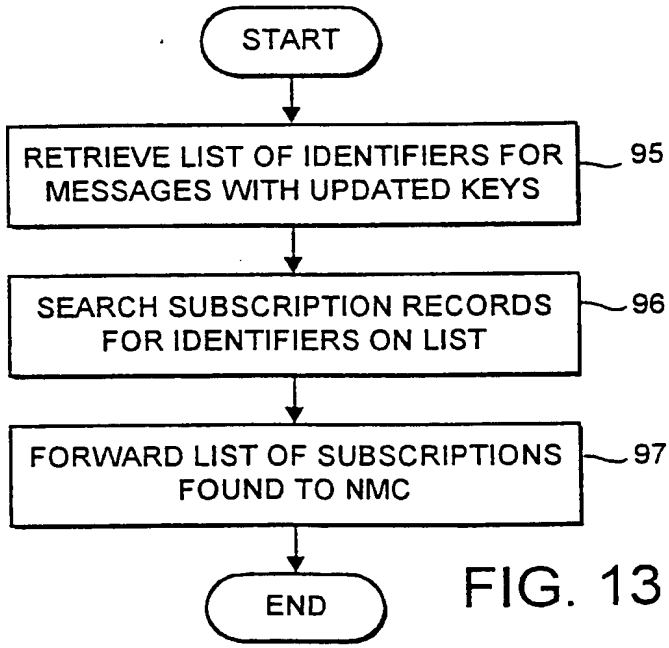

START
RETRIEVE LIST OF IDENTIFIERS FOR MESSAGES WITH UPDATED KEYS
95
SEARCH SUBSCRIPTION RECORDS FOR IDENTIFIERS ON LIST
96
FORWARD LIST OF SUBSCRIPTIONS FOUND TO NMC
97
END

FIG. 13

INTERNATIONAL SEARCH REPORT

Inter ɔnal Application No
PCT/GB 98/02064

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04Q7/22 H04Q7/32

According to International Patent Classification(IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 96 41493 A (ERICSSON TELEFON AB L M) 19 December 1996	1,2,6, 13-16, 18-21,25
Y	see page 40, line 5 - page 41, line 2 see page 52, line 20 - page 53, line 17 see page 55, line 10 - line 17 see page 57, line 19 - page 58, line 6 see claims 1-10 --- -/--	3,7,8, 12,17,22

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
10 November 1998	18/11/1998

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Baas, G

2

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Inter ɔnal Application No
PCT/GB 98/02064

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	FARRUGIA A J ET AL: "SMART CARD TECHNOLOGY APPLIED TO THE FUTURE EUROPEAN CELLULAR TELEPHONE ON THE DIGITAL D-NETWORK" SELECTED PAPERS FROM THE SECOND INTERNATIONAL SMART CARD 2000 CONFERENCE, 4-6 OCTOBER 1989, AMSTERDAM, NL, 1 January 1989, pages 95-107, XP000472724 see page 100, line 1 - page 103, line 21 ---	3,7,8, 12,22
Y	US 5 371 493 A (SHARPE ANTHONY K ET AL) 6 December 1994 see column 3, line 3 - line 10 see column 6, line 35 - line 42 ---	17
A	EP 0 689 368 A (PTT GENERALDIREKTION) 27 December 1995 -----	

2

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inter nal Application No
PCT/GB 98/02064

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9641493 A	19-12-1996	US 5768276 A	16-06-1998
		AU 6020296 A	30-12-1996
US 5371493 A	06-12-1994	DE 69219991 D	03-07-1997
		DE 69219991 T	27-11-1997
		EP 0538933 A	28-04-1993
		JP 5218946 A	27-08-1993
		SG 48347 A	17-04-1998
EP 0689368 A	27-12-1995	AT 153206 T	15-05-1997
		AU 691271 B	14-05-1998
		AU 2174595 A	04-01-1996
		BR 9508091 A	12-08-1997
		CA 2152215 A	21-12-1995
		WO 9535635 A	28-12-1995
		CN 1128476 A	07-08-1996
		CZ 9603513 A	14-05-1997
		DE 59402759 D	19-06-1997
		DK 689368 T	08-12-1997
		ES 2103557 T	16-09-1997
		FI 965078 A	17-12-1996
		GR 3023908 T	30-09-1997
		HU 76397 A	28-08-1997
		JP 8265843 A	11-10-1996
		NO 965315 A	18-02-1997
		NZ 287390 A	19-12-1997
		PL 317643 A	14-04-1997
		SG 34235 A	06-12-1996
		SI 9520064 A	30-04-1997
		SK 161396 A	05-11-1997
		ZA 9505091 A	10-04-1996